Radványi Tibor
Eszterházy Károly Főiskola
radvanyi.tibor@ektf.hu

KRIPTOGRÁFIAI ALGORITMUSOK ALKALMAZÁSA A RÁDIÓFREKVENCIÁS AZONOSÍTÁS ÉS KOMMUNIKÁCIÓ SORÁN

Absztrakt

Ebben a cikkben egy lendületesen fejlődő, a mindennapokban egyre több helyen megtalálható technológiával, az RFID technológiával fogunk foglalkozni. Bemutatjuk, hogy milyen lehetőségek vannak a rendszer különböző szintjeinek a támadására. A támadások részletes vizsgálata lehetőséget ad arra, hogy a védekezést jobban felépíthessük. Kitérünk arra, hogy milyen védekezési lehetőségeink vannak az egyes szinteken. A legfőbb cél a tag-ek és a tag-ekben tárolt adatok védelme. Megvizsgáljuk, hogy milyen kriptográfiai eljárásokat, algoritmusokat lehet alkalmazni. Ezen algoritmusok alkalmazhatósága erősen függ az RFID tag-ek felépítésétől, a bennük megjelenő számítási kapacitás mértékétől és az implementált memória méretétől. Nagy kihívást jelent az olcsó, várhatóan robbanásszerűen elterjedő passzív tag-ekben tárolt adatok megfelelő védelme.

Kulcsszavak: RFID, adatbiztonság, kriptográfia, adatvédelem, UHF, HF/NFC

Bevezetés

Napjainkban széles körben megtalálhatóak az azonosítási rendszerek különböző formái. Egy olyan kód– és kommunikációs rendszert értünk ez alatt, amely személyeket, tárgyakat, eseményeket egyedileg azonosít. A legfiatalabb és legdinamikusabban fejlődő azonosítási módszer az RFID. Különböző típusú szenzorokkal illetve helymeghatározó rendszerekkel párosítva széles felhasználási területen alkalmazható. Találkozhatunk vele az autógyártásban, logisztikában, gyógyszer- és hadiiparban valamint számos más helyen is. Lehetővé teszi a közúti, légi és vízi szállítás teljes nyomon követését, és nem utolsó sorban ellenőrizhetővé válik annak minőségi állapota a szállítás folyamán. A technológia azonosítási- és biztonsági lehetőségeit egyre inkább kihasználják a modern útlevelek, a digitális azonosítók és nem utolsó sorban még a legújabb fizetési megoldások is. [1][2]

Egy termék számtalan veszélynek van kitéve, ameddig a gyártótól el nem jut a fogyasztóhoz. A gyárból átkerül egy átmeneti raktárba, innen a nagykereskedő, majd a kiskereskedelmi cég elosztó központjába, végül pedig az áruházak polcaira. Ez elég hosszú folyamat, amely során az áruk elveszhetnek, összecserélődhetnek, ellophatják őket.

Magyarországon jelenleg is folynak az egyeztetések a mobillal való fizetési lehetőségekről, melynek elterjedése egy hatalmas mérföldkő lehet a fejlődésben. A felhasználók nincsenek tisztában ennek veszélyeivel, legtöbbjük nem tud, vagy nem is akar foglalkozni ehhez hasonló problémákkal. Így a gyártóknak folyamatosan figyelniük

kell a biztonságra, figyelemmel kell követniük azokat a lehetőségeseket, melyek bármilyen sérülést, vagy adatlopást tudnánk okozni a felhasználót körülvevő rendszerekben. A csökkenő előállítási költségek révén az olcsó passzív RFID rendszerekre jellemző adattárolási limit is előbb vagy utóbb megszűnik. Felválthatják az aktív címkék, melyek már sokkal nagyobb biztonsággal használhatóak, és nem kell speciális algoritmusokat kidolgozni, hogy működni tudjanak az egyszerűbb rendszereken is.

Végül is hamar belátták azt, hogy első szempont mindig az információkezelés biztonságos és akadálymentes kezelése legyen, s a hatékonyságot ezzel a háttérbe szorították. Véleményünk szerint is a legfontosabb az adatok biztonságban tartása, főként az olyan rendszerek esetében, ahol nélkülözhetetlen a titoktartás. Pl. egy banki szolgáltatás inkább legyen lassabb, és biztonságosabb, mint legyen gyors. [3][10]

Támadás az RF interface-en keresztül

Az RFID rendszerek elleni egyik jellemző támadási módszer az RF interfészen keresztül érkező támadás. Az RFID rendszerek rádió rendszerek és elektromágneses hullámok segítségével kommunikálnak közelre és távolra egyaránt. Így a támadónak lehetősége van a rádiófrekvenciás interfészen keresztül is támadást indítani, mivel nincs szükség az olvasó vagy a transzponder fizikai hozzáféréshez. Ennek a támadástípusnak számos alesete ismert, a következőkben ennek bemutatására teszek kísérletet. [11,12,13,14]

Nagy hatótávolságú RFID rendszernek nevezzük azt, melyben a két eszköz közötti távolság nagyobb, mint 1 méter. Általában UHF (868 - 915 MHz) vagy mikrohullámú frekvenciatartományban (2,4 vagy 5,8 GHz) működnek. Ha a tag kikerül a rendszer olvasási tartományából, szintén két lehetőség merül fel az adás megszakítására. Az egyik ok, hogy a tag nem kap elég áramot az antennából a működéshez. A másik lehetőség pedig, ha a visszavert teljesítmény kevés ahhoz, hogy az olvasó érzékelni tudja. A távolság növeléséhez emelni kell az olvasó átviteli teljesítményét. Ahhoz, hogy az olvasási távolság a kétszeresére nőjön az olvasó teljesítményét a négyszeresére kell emelni. Ha szeretnénk megtartani a visszaszórás teljesítményének mértékét kétszeres olvasási távolságon, akkor az olvasót teljesítményét már tizenhatszorosára kellene növelni. 2005-ben sikerült a Yagi-Uda antennával 21 méterről sikeres támadást végrehajtani. [4][10]

A lehallgatás (eavesdropping)

A kommunikáció lehallgatása az olvasó és a transzponder között történik. Az RFID rendszerek hatótávolsága pár centimétertől (pl.: 13,56 MHz) több méterig terjedhet (pl: 868 MHz). Finke and Kelter megállapították, hogy 13,56 MHz-es induktív csatolású rendszer, akár 3 méterről is lehallgatható.[4] A vevő pár kHz-es sávszélességen az olvasó modulálatlan jelét több 100 méterről is érzékelheti. Nagyobb távolságnál a jelet zavarhatják fém tárgyak, mint például kerítések, alumínium tárgyak, de akár nagyobb épületek is torzíthatják. Mitől függ, hogy a támadó sikeresen lehallgassa az eszközeink (olvasó és transzponder) közötti kommunikációt? A befolyásoló tényezők száma nagyon nagy. [7][8]

- Függ a RF tér karakterisztikájától. Ezt az olvasó antennájának geometriája, belső felépítése és a kibocsájtási energia határozza meg.
- Fontos tényező az olvasó és a transzponder közötti térben elhelyezkedő zavaró tárgyak, fém felületek mérete, elhelyezkedése.
- Befolyásolja a támadó lehallgató eszközének minősége, felépítése, geometriája. Nagyban függ az olvasó által kibocsájtott, generált tér energiájától.
- Fontos befolyásoló tényező, hogy az RF kommunikációban passzív vagy aktív transzponderek vesznek részt. Ha a tag passzív, akkor az olvasó által gerjesztett tér energiáját használja, így a visszasugárzott, hasznos információ alacsonyabb energiával vesz részt a kommunikációban. Ez az UHF tag-ek esetében (868 MHz – 915 MHz) 1–3 méter. Amennyiben a tag aktív, esetleg szemipasszív, azaz rendelkezik saját energiaforrással, az e távolság megnőhet akár 10–30 méterre is. Aktív esetben a tag által kisugárzott információ nagyobb energiája miatt könnyebben fogható a támadó eszközeivel. Illetve ez az eszköz a nagyobb támadási térben jobban rejtve maradhat. Támadási térnek nevezzük azt a térrészt, ahol a támadó adott jellemzőkkel rendelkező lehallgató eszközét elhelyezve, még sikeres támadást tud végrehajtani.

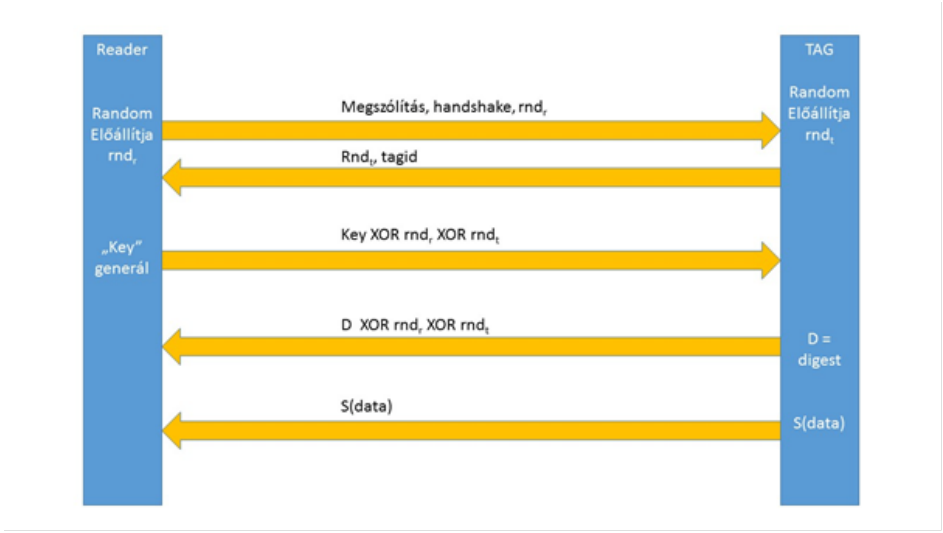
A lehallgatás során az adatokat a következő támadások érhetik:

- Titkos vagy személyes adat kerül illetéktelen kézbe. Ekkor a kommunikációra nincs hatással a támadó. A jelenlétét nagyon nehéz, ha nem lehetetlen felfedezni. Ebben az esetben az adatok közvetlen védelme, kriptográfiai protokollok használata segíthet.
- A lehallgatott adatot a támadó megváltoztatja és a megváltoztatott, hamis adat jut el az olvasóhoz. Nehezen megvalósítható, komoly támadó eszközt feltételező támadás. Az adat módosításhoz szükséges időablaknak be kell férnie a kommunikációs adatcsere folyamatába.
- Egy másik lehetőség, hogy ha a támadó nem módosítja a lehallgatott adatot, hanem a helyére új adatot szúr be. Ez akkor lehetséges, ha a transzponder viszonylag sok adatot küld az olvasónak. Így a kommunikációra sok idő szükséges. A fenti támadási módok esetén a támadót felfedezhetik, az adatait kivédhetik. Ellenőrző összegek használata és a kriptográfiai algoritmusok és protokollok kombinálása lehetővé teszi ezt.
- A lehallgatásos támadás egy bonyolultabb, komoly technikai felkészülést igénylő módja a „relay attack” támadás. Ebben az esetben a támadó nem csak lehallgatja a kommunikációt, hanem a megszerzett adatokat egy másik csatornán pl. wifi nagyobb távolságra továbbíthatja. A másik helyen egy eszközzel az adatok felhasználásra kerülhetnek pl egy vásárlás során. Ezt a támadási módot nehéz kivédeni az érintésmentes fizetési lehetőségek tulajdonságai miatt. Egyelőre jó lehetőséget biztosít az egyéb azonosítóval való kiegészítése a folyamatnak. A legegyszerűbb a pin kód használata, de bármely személyhez, helyhez kötött biometrikus azonosító is kiváló lehet. [15][16]

Láthatjuk, hogy a lehallgatás bizonyos esetekben könnyen elvégezhető támadási mód. Viszonylag sok lehetőséget tartalmaz a támadó számára és elég nehéz észlelni és kivédeni.

Az adatok védelme érdekében, ha nem tudjuk megvédeni a kommunikációs csatornát, akkor az esetlegesen lehallgatott információt tegyük nem vagy csak nehezen

felhasználhatóvá a támadó számára. Ehhez nyújt segítséget, ha kriptográfiai protokollt használunk az információváltás során.



1. ábra: Reader és transzponder kommunikáció

Biztonsági lépések

A rejtjelezés alapvetően a passzív támadások ellen véd, az aktív támadások elleni védekezéshez kriptográfiai protokollokat használunk, ami előre meghatározott üzenetcsere-folyamatot jelent. Ennek során észleljük az aktív támadásokat, és kivédjük azok káros következményét.
A publikált protokolloknak sok közös vonásuk van. [6] Fő lépéseik:

1. Az olvasó kérést sugároz a tag-nek
2. A tag azonosítja magát az olvasónak (megadja a tárolt adatokat)
3. Az olvasó továbbítja az adatokat a háttér szervernek
4. A szerver adatbázisa alapján feldolgozza az adatokat
5. A szerver elküldi a hitelesítést és a feldolgozott adatot

A különbség a különböző szinteken kriptográfiai primitívek alkalmazásában van. [5] A tag kódolja az adatokat mielőtt továbbítja az olvasónak. A háttér szerver a közös kulccsal visszafejti az üzenetet, adatbázisában megkeresi és feldolgozza azt.

A lehallgatás ellen az 1, 2 pontok által leírt folyamatot kell részleteznünk és erősíteni. Lehetséges az erős védelmi rendszerbe bevonni a háttér szervert is. Így két lehetőségünk adódik. Az egyik, amikor a kriptográfiai protokoll mindhárom réteget érinti, azaz a transzpondert, az olvasót és a háttérszervert is. A másik lehetőség, hogy próbáljuk a tag és az olvasó közötti kommunikációra szorítani a védelmet, feltételezve, hogy az olvasó és a háttérszerver közötti, többnyire belső, védett hálózatban futó adatforgalom már biztonságban van.

Természetesen erősen függ a követető protokoll attól, hogy a kommunikációban passzív vagy aktív tag-ek szerepelnek. Már a meglévő követelmények is eltérnek, és a rendelkezésre álló számítási kapacitás is jelentős különbséget mutat.

Tekintsük át az 1. ábrán is szemléltetett kommunikációs sémát.

Látható, hogy a titkosításhoz egyrészt XOR függvényt használunk, ami könnyen implementálható hardver szinten is, így a passzív tag-ben nincs akadálya a használatának.

A XOR protokoll különböző kulcsokat használ, különböző irányban. [17,18]

$$R \rightarrow T : x \oplus k1$$
$$T \rightarrow R : x \oplus k2$$

Biztonságos megoldás, hogy a k1 és k2 kulcsokat véletlenszerűen választjuk minden egyes futtatáskor. Az egyik lehetőség ennek megvalósítására a XOR kulcsgenerálás, melyben i változó alapján R véletlenszerűen választ új k(i) kulcsot és XOR titkosítást hajt végre a k(i-1) kulccsal. Ezáltal a következő protokollt kapjuk:

$$R \rightarrow T : a(i) = x(i) \oplus k(i), k(i) \quad k(i-1)$$
$$T \rightarrow R : b(i) = x(i) \oplus k(0)$$

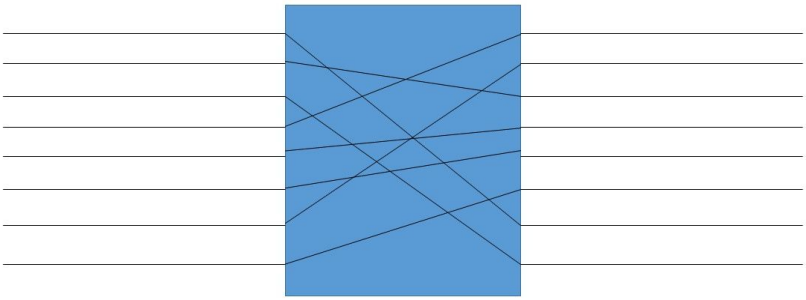
ahol i = 2,3,… egy számláló, minden futásnál egyel növelve. x(i) az i-edik véletlenszám és k(0) és k(1) előre beállított osztott kulcsok. k(1), k(2), … sorozat nem változik véletlenszerűen, csak az értéküket nem tudja követni a támadó.

Valamint megjelenik egy S függvény, amit kicsit részletezni szükséges.

Először tekintsük az úgynevezett P és S dobozokat. Ezek alapjait képezik a kriptográfiai algoritmusoknak. Előnyük, hogy elektrotechnikailag könnyen megvalósíthatóak. Így a passzív tag-ek rendkívül korlátozott eszközkészletéhez is integrálhatóak lesznek. Aktív tag-ek esetén ez nem jelent gondot, hiszen a tag tartalmaz intelligenciát, azaz programozható processzort, így a teljes AES algoritmus megvalósítható viszonylag kis energia ráfordítással és rövid idő alatt.

A passzív tag-ek esetén használjuk a P és S dobozok kombinációját.

A P doboz egy 8 bit bemenő adatból 8 bit kimenő adatot előállító függvény. Egy gyors és egyszerű elektronikai eszköz, mely ha ismerjük a P doboz hozzárendelési szabályát, akkor az inverz függvény is elkészíthető. A feladata a 8 bit valamilyen keverése, egy bitpermutáció előállítása.



2. ábra: egyféle P doboz leképezés

Az S dobozok egy 6 bemenő bitből 4 bitet előállító nem lineáris függvényt megvalósító eszközök. [19] Az S dobozok működését egy 4 sorból és 16 oszlopból álló táblázat írja le. Minden egye S doboznak más és más a táblázata. Ezek felhasználásával lehetséges az S dobozok kódolása. A bejövő 6 bit első és hatodik bitje adja a sorindexet, míg a 4 középső bitnek megfelelő decimális szám az oszlopindexet. Így kapjuk a kimenő 4 bitet a táblázat megfelelő cellája alapján.

	0000	0001	0010	0011	0100	0101	0110	0111	1000	1001	1010	1011	1100	1101	1110	1111
00	0010	1100	0100	0001	0111	1010	1011	0110	1000	0101	0011	1111	1101	0000	1110	1001
01	1110	1011	0010	1100	0100	0111	1101	0001	0101	0000	1111	1010	0011	1001	1000	0110
10	0100	0010	0001	1011	1010	1101	0111	1000	1111	1001	1100	0101	0110	0011	0000	1110
11	1011	1000	1100	0111	0001	1110	0010	1101	0110	1111	0000	1001	1010	0100	0101	0011

3. ábra: egyféle S doboz leképezés

Az 1. ábrán látható S függvény, mely előállítja a user memória tartalmának S(data) képét, és elküldi az olvasónak, egy S és P dobozokból álló összetett függvény. A használt S és P dobozok táblázatait ismerve az

$$S\text{-}1(S(data)) = data$$

alapján visszakapjuk a tag-ben tárolt adatot. Hogy melyik S és P dobozt használjuk, azt a reader által küldött key kulcs fogja meghatározni. A reader egy célszámítógép, mely minden olyan számítási kapacitással és tárral rendelkezik, mely szükséges a kulcs előállítására és a kapott S(data) visszafejtésére. A tag-ek az S dobozok és a P dobozok elektronikus megvalósításait.

Az ellenőrzéshez a tárolt data-ról egy lenyomatot, „digest”-et készítünk. Ehhez kiválóan megfelelnek a közismert HASH függvények. A tag-ekben implementáljuk a HASH függvények egyikét, pl a MD5 függvényt. Ennek alkalmazásával lehetséges az

elküldött, titkosított adat visszafejtés utáni változatlanság ellenőrzése. Egy plusz védelmet nyújt az adatváltoztató, esetleg adat beszúrásával élő támadások ellen.

Következtetés

Az RFID rendszerek használata napjainkban is folyamatosan változik. Számos új technológia jelenik meg és a gyártók, multinacionális cégek törekednek arra, hogy ezeket az újdonságokat eljutassák a felhasználókig. A transzponderek napról napra egyre kisebb kivitelben és olcsóbban kerülnek ki a gyárakból, mely szintén segíti annak elterjedését. A széles körű elterjedésnek köszönhetően, egyre több szegmensben találhatóak meg ezek a rendszerek, így annak veszélyeire, sebezhetőségeire is sokkal nagyobb hangsúlyt kell fektetni.

A fent vázolt rendszer alapot biztosíthat az egyszerű, olcsó transzponderek hordozta adatok védelmére. Hozzátéve, hogy ennek alkalmazásához meg kell változtatni a jelenleg használt Class1Gen2 tag-ek protokollját, és be kell építeni a megfelelő kommunikációs és S illetve P dobozokat megvalósító részeket.

Irodalomjegyzék

[1] Dr. Imre Sándor, Kis Zoltán, Molnár László, Pogátsa Attila, Schulcz Róbert, Tóth Gábor – RFID rendszerek vizsgálata felhasználás és technológia szempontjából http://www.rfid.answare.hu:8080/site/kutatasi-erdmenyeink/radios-megoldasok/2006/rfid-rendszerek-vizsgalata-felhasznalas-es-technologia-szempontjabol.pdf/view.

[2] Klaus Finkezeller – RFID Handbook, Third Edition, 2010

[3] Pedro Peris-Lopez, Julio Cesar Hernandez-Castro, Juan M. Estevez Tapiador and Arturo Ribagorda – LMAP: A Real lightweight Mutual Authentication Protocol for Low-cost RFID tags http://events.iaik.tugraz.at/rfidsec06/program/papers/013%20-%20lightweight%20mutual%20authentication.pdf

[4] Hee-Jin Chae, Daniel J. Yeager, Joshua R. Smith, and Kevin Fu (University of Massachusetts) Maximalist Cryptography and Computation on the WISP UHF RFID Tag 2007

[5] Sindhu Karthikeyan and Mikhail Nesterenko_Kent State University, RFID Security without Extensive Cryptography 2005

[6] M. McLoone and M.J.B. Robshaw (Queen's University, Belfast, U.K.) Public Key Cryptography and RFID Tags 2008

[7] Ernst Haselsteiner, Klemens Breitfuß: Security in Near Field Communication (NFC) Philips SemiconductorsMikronweg 1, 8101 Gratkorn, Austria

[8] Radványi Tibor, Biro Csaba, Király Sándor: RFID tagek elleni támadás és a védekezés lehetőségei, Attack against the RFID tags and possibilities of the defense, Networkshop 2014 Pécs, , ISBN: 978-963-88335-5-6, elektronikus kiadás.

[9] Radványi Tibor, Bíró Csaba: Az adatvédelem helyzete az RFID-ban, SzamOkt 2013. október 10-13, Nagyszeben (Sibiu, Románia), ISSN 1842-4546 283-289 oldal

[10] Jung-Sik Cho, Sang-Soo Yeo, Sung Kwon Kim: Securing against brute-force attack: A hash-based RFID mutual authentication protocol using a secret value, Computer Communications 34 (2011) 391–397

[11] A. Juels, RFID security and privacy: a research survey, Selected Areas in Communications 24 (2) (2006) 381–394. February.

[12] S.S. Yeo, S.K. Kim, Scalable and flexible privacy protection scheme for RFID systems, European Workshop on Security and Privacy in Ad hoc and Sensor Networks – ESAS'05 LNCS, 3813, Springer, 2005, pp. 153–163.
[13] S. Weis, S. Sarma, R. Rivest, D. Engels, Security and privacy aspects of low-cost radio frequency identification systems, in: International Conference on Security in Pervasive Computing, March 2003, pp. 201–212
[14] S.A. Sarma, S.E. Weis, D.W. Engels, RFID systems and security and privacy implications, cryptographic hardware and embedded systems – CHES 2002, LNCS, vol. 2523, Springer, 2002. August, pp. 454–469.
[15] S. Yu, K. Ren, W. Lou, A privacy-preserving lightweight authentication protocol for low-cost RFID tags, in: IEEE MILCOM 2007, October 2007, pp. 1–7.
[16] Y.-C. Lee, Y.-C. Hsieh, P.-S. You, T.-C. Chen, An improvement on RFID authentication protocol with privacy protection, in: Third International Conference on Convergence and Hybrid Information Technology – ICCIT 2008, vol. 2, November 2008, pp. 569–573.
[17] Jeongkyu Yang, Jaemin Park, Hyunrok Lee, Kui Ren, Kwangjo Kim (KOMSCO, ICU, WPI Mutual Authentication Protocol for Low-cost RFID 2005
[18] NIST. Recommendation for block cipher modes of operation: Galois/counter mode (GCM) and GMAC. NIST Special Publication 800-38D, 2007.
[19] Lauren De Meyer, Beg Bilgin, and Bart: Extended Analysis of DES S-boxes, Proceedings of the 34rd Symposium on Information Theory in the Benelux, 30-31 May University Press.